Industry Recognized Credential Transfer Assurance Guide: Cisco I, II, and III CCNA 7

Cisco Certified Network Associate (CCNA)

April 13, 2022

Industry Recognized Credential Transfer Assurance Guides (ITAGs) are a statewide transfer initiative that guarantees the award of college-level credit to students earning agreed-upon, industry recognized credentials. Students meeting credentialing requirements, regardless of where the learning was achieved, will be eligible to earn credit for specified courses deemed equivalent to the stated industry recognized credential listed on the ITAG document. Credentials are reviewed and aligned to postsecondary learning outcomes that are endorsed by Ohio's public institutions of higher education. The receiving institution must offer an equivalent course or program. Additional information on accessing and awarding ITAG credit is outlined in this document.

Required Credential(s)

Credential Name: Cisco Certified Network Associate (CCNA)

Credential Issuer: Cisco

Exam(s): Exam # 200-301

Additional Requirements for Credit: CCNA credential must be current. CCNA credential will award credit to students for Cisco I, Cisco II, and Cisco III courses.

Credit Access and Verification

Student: Students seeking credit should use the Cisco Certification Tracking System to email credential verification to the institution. The tracking system can be found at the following website: https://cloudsso.cisco.com/idp/prp.wsf?wa=wsignin1.0&wtrealm=https://www.certmetrics.com/cisco/login.aspx

Institution: Receiving institutions should request that the student send an email verification through the Cisco Certification Tracking System.

Course Information

Course Name: Cisco I CCNA 7: Introduction to Networks – ITITN017

Credit Hours: 3-4

Course Description: Introduction to Networks (ITN) covers the architecture, structure, functions and components of the Internet and other computer networks. Students achieve a basic understanding of how networks operate and how to build simple local area networks (LAN), perform basic configurations for routers and switches, and implement Internet Protocol (IP).

Course Information *(cont.)*

Course Information

Course Name: Cisco II CCNA 7: Switching, Routing, and Wireless Essentials (SRWE) – ITITN018

Credit Hours: 3-4

Course Description: Switching, Routing, and Wireless Essentials (SRWE) covers the architecture, components, and operations of routers and switches in small networks and introduces wireless local area networks (WLAN) and security concepts. Students learn how to configure and troubleshoot routers and switches for advanced functionality using security best practices and resolve common issues with protocols in both IPv4 and IPv6 networks.

Course Information

Course Name: Cisco III CCNA 7: Enterprise Networking, Security, and Automation (ENSA) – ITITN019

Credit Hours: 3-4

Course Description: Enterprise Networking, Security, and Automation (ENSA) describes the architecture, components, operations, and security to scale for large, complex networks, including wide area network (WAN) technologies. The course emphasizes network security concepts and introduces network virtualization and automation. Students learn how to configure, troubleshoot, and secure enterprise network devices and understand how application programming interfaces (API) and configuration management tools enable network automation.

Learning Outcomes and Credential Alignment

Alignment of Cisco Certified Network Associate Exam Content to Postsecondary Learning Outcomes for Cisco I

Postsecondary Learning Outcomes *(Copy of CTIT017)*	Content from Credential
1. Configure switches and end devices to provide access to local and remote network resources.	• Configure initial settings on a Cisco switch. • Configure switch ports to meet network requirements. • Configure secure management access on a switch. • Explain how LANs and WANs interconnect to the internet. • Identify some basic security threats and solution for all networks. • Explain how to access a Cisco IOS device for configuration purposes. • Explain how to navigate Cisco IOS to configure network devices. • Configure a Cisco IOS device using CLI. • Configure a host device with an IP address. (PC/Client) • Verify connectivity between two end devices. • Frame Forwarding • Switching Domains • Access ports (data and voice) • Default VLAN • Describe remote access and site-to-site VPNs.
2. Explain how physical and data link layer protocols support the operation of Ethernet in a switched network.	• Explain the role and function of network components • Describe the Ethernet MAC address. • Explain how a switch builds its MAC address table and forwards frames. • Describe switch forwarding methods and port settings available on Layer 2 switch ports. • Describe characteristics of network topology architectures • Identify interface and type of cables and cables issues (collisions, errors, mismatch duplex, and/or speed) • Describe switching concepts

Learning Outcomes and Credential Alignment *(cont.)*

3. Configure routers to enable end-to-end connectivity between remote devices.	• Configure device access control using local passwords • Describe remote access and site-to-site VPNs • Configure and verify access control lists • Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
4. Create IPv4 and IPv6 addressing schemes and verify network connectivity between devices.	• Configure and verify IPv4 addressing and subnetting • Describe the need for private IPv4 addressing Configure and verify IPv4 and IPv6 static routing • Explain the role of the major header fields in the IPv4 packet. • Explain the role of the major header fields in the IPv6 packet. • Explain how network devices use routing tables to direct packets to a destination network. • Explain the function of fields in the routing table of a router.
5. Explain how the upper layers of the Open Systems Interconnect (OSI) model support network applications.	• Explain the role and function of network components within the Layer.
6. Configure a small network with security best practices.	• Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) • Describe security program elements (user awareness, training, and physical access control) • Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics) • Differentiate authentication, authorization, and accounting concepts
7. Troubleshoot connectivity in a small network.	• Describe the purpose of first hop redundancy protocol • Explain the role of DHCP and DNS within the network • Configure and verify DHCP client and relay

Learning Outcomes and Credential Alignment

Alignment of Cisco Certified Network Associate Exam Content to Postsecondary Learning Outcomes for Cisco II

Postsecondary Learning Outcomes *(Copy of CTIT018)*	Content from Credential
1. Configure Virtual Local Area Network (VLANs) and Inter-VLAN routing applying security best practices.	• Configure and verify VLANs (normal range) spanning multiple switches • Configure VLAN in multi- Switched Environment and verify interswitch connectivity • Configure Dynamic Trunking Protocol (DTP). • Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP). • Access ports (data and voice) • Default VLAN • Connectivity • Configure and verify interswitch connectivity • Trunk ports • 802.1Q • Native VLAN • Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP) • Configure router-on-a-stick inter-VLAN routing • Spanning Tree Protocol (STP) Operations • Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations • Root port, root bridge (primary/secondary), and other port names • Port states (forwarding/blocking) • PortFast benefits • Compare Cisco Wireless Architectures and AP modes • Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG) • Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS) • Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

Learning Outcomes and Credential Alignment *(cont.)*

2. Troubleshoot inter-VLAN routing on Layer 3 devices.	• Configure and verify (Layer 2/Layer 3) EtherChannel (LACP) • EtherChannel Operation • Configuring EtherChannel • Verify and Troubleshoot EtherChannel • Troubleshoot common inter-VLAN configuration issues.
3. Configure redundancy on a switched network using Spanning Tree Protocol (STP) and Port Link Aggregation (EtherChannel).	• Explain common problems in a redundant, L2 switched network. • Explain how STP operates in a simple switched network. • Explain how Rapid PVST+ operates. • Describe EtherChannel technology. • Configure and troubleshoot redundancy on a switched network using STP and EtherChannel. • Speed and duplex • VLAN match • Range of VLANs
4. Troubleshoot Port Link Aggregation (EtherChannel) on switched networks.	• Verify and Troubleshoot EtherChannel • Configure EtherChannel. • EtherChannel support. • View the EtherChannel Summary Information. • View Port Channel Configuration. • Correct the Misconfiguration.
5. Explain how to support available and reliable networks using dynamic addressing and first-hop redundancy protocols.	• Describe the purpose of first hop redundancy protocol.

Learning Outcomes and Credential Alignment *(cont.)*

6. Configure dynamic address allocation in IPv6 networks.	• Compare static and dynamic routing concepts. • Describe the structure of a routing table. • Explain how routers determine the best path. • Compare static and dynamic routing concepts. • Explain how an IPv6 host can acquire its IPv6 configuration. • Explain the operation of SLAAC. • Explain the operation of DHCPv6. • Configure a stateful and stateless DHCPv6 server.
7. Configure WLANs using Wireless LAN Controllers (WLC) and L2 security best practices.	• Describe wireless principles. • Nonoverlapping Wi-Fi channels. • SSID. • RF. • Encryption. • Configure the components of a wireless LAN access for client connectivity using GUI only. • Remote Site WLAN Configuration. • Configure a Basic WLAN on the WLC • Configure a WPA2 Enterprise WLAN on the WLC. • Troubleshoot WLAN Issues. • Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS). • WLAN creation, security settings, QoS profiles, and advanced WLAN settings. • Describe wireless security protocols (WPA, WPA2, and WPA3). • Configure WLAN using WPA2 PSK using the GUI.
8. Configure switch security to mitigate local area network (LAN) attacks.	• Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques) • Describe security program elements (user awareness, training, and physical access control) • Configure device access control using local passwords • Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics) • Implement Port Security

Learning Outcomes and Credential Alignment *(cont.)*

	• Mitigate VLAN Attacks • Mitigate DHCP Attacks • Mitigate ARP Attacks • Mitigate STP Attacks
9. Configure IPv4 and IPv6 static routing on routers.	• Describe the command syntax for static routes. • Configure IP Static Routes • Configure IP Default Static Routes • Configure Floating Static Routes • Configure Static Host Routes (Configure IPv4 and IPv6 static host routes that direct traffic to a specific host). • Routing protocol • Network mask • Next hop • Administrative distance • Metric • Gateway of last resort • Compare IPv6 address types • Global unicast • Unique local • Link local • Anycast • Multicast • Modified EUI 64

Learning Outcomes and Credential Alignment

Alignment of Cisco Certified Network Associate Exam Content to Postsecondary Learning Outcomes for Cisco III

Postsecondary Learning Outcomes *(Copy of CTIT019)*	Content from Credential
1. Configure single-area Open Shortest Path First (OSPFv2) in both point-to-point and multiaccess networks.	• Describe basic OSPF features and characteristics. • Describe the OSPF packet types used in single-area OSPF. • Explain how single-area OSPF operates. • Configure and verify single area OSPFv2. • Neighbor adjacencies. • Configure single-area OSPFv2 in a point-to-point network. • Configure the OSPF interface priority to influence the DR/BDR election in a multiaccess network. • Implement modifications to change the operation of single-area OSPFv2. • Broadcast (DR/BDR selection). • Router ID. • Describe the purpose of first hop redundancy protocol.
2. Explain how to mitigate threats and enhance network security using access control lists and security best practices.	• Describe the current state of cybersecurity and vectors of data loss. • Describe tools used by threat actors to exploit networks. • Describe malware types. • Describe common network attacks. • Explain how IP vulnerabilities are exploited by threat actors. • Explain how TCP and UDP vulnerabilities are exploited by threat actors. • Explain how IP services are exploited by threat actors. • Describe best practices for protecting a network. • Describe common cryptographic processes used to protect data in transit. • Explain how ACLs filter traffic. • Explain how ACLs use wildcard masks. • Explain how to create ACLs. • Compare standard and extended IPv4 ACLs. • Configure and verify access control lists.

Learning Outcomes and Credential Alignment *(cont.)*

3. Implement standard IPv4 Access Control List (ACL) to filter traffic and secure administrative access.	• Configure standard IPv4 ACLs to filter traffic to meet networking requirements. • Modify IPv4 ACLs • Secure VTY Ports with a Standard IPv4 ACL • Configure Extended IPv4 ACLs (Configure extended IPv4 ACLs to filter traffic according to networking requirements). • Configure device access control using local passwords. • Differentiate authentication, authorization, and accounting concepts.
4. Configure Network Address Translation (NAT) services on the edge router to provide IPv4 address scalability.	• NAT Characteristics (Explain the purpose and function of NAT). • Explain the operation of different types of NAT. • Describe the advantages and disadvantages of NAT. • Configure static NAT using the CLI. • Configure dynamic NAT using the CLI. • Configure PAT using the CLI. • Describe NAT for IPv6. • Configure and verify inside source NAT using static and pools.
5. Explain techniques to provide address scalability and secure remote access for WANs.	• Purpose of WANs • WAN Operations • Compare traditional WAN connectivity options. • Compare modern WAN connectivity options. • Compare internet-based connectivity options. • Describe the benefits of VPN technology. • Describe different types of VPNs. • Explain how the IPsec framework is used to secure network traffic. • Configure and verify inside source NAT using static and pools • Explain the role of DHCP and DNS within the network • Configure network devices for remote access using SSH

Learning Outcomes and Credential Alignment *(cont.)*

6. Explain how to optimize, monitor, and troubleshoot scalable network architectures.	• Network Documentation (Explain how network documentation is developed and used to troubleshoot network issues). • Compare troubleshooting methods that use a systematic, layered approach. • Describe different networking troubleshooting tools. • Determine the symptoms and causes of network problems using a layered model. • Troubleshoot a network using the layered model. • Explain the function of SNMP in network operations. • Troubleshoot common static and default route configuration issues. • Configure a floating static route to provide a backup connection. • Configure and verify DHCP client and relay • Explain how automation impacts network management. • Pare traditional networks with controller-based networking. • Describe controller-based and software defined architectures (overlay, underlay, and fabric). • Separation of control plane and data plane. • North-bound and south-bound APIs. • Compare traditional campus device. management with Cisco DNA Center enabled device management.
7. Explain how networking devices implement Quality of Services (QoS).	• Explain how network transmission characteristics impact quality. • Describe minimum network requirements for voice, video, and data traffic. • Describe the queuing algorithms used by networking devices. • Describe the different QoS models. • Explain how QoS uses mechanisms to ensure transmission quality. • Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping.
8. Implement protocols to manage the network.	• Device Discovery with CDP • Device Discovery with LLDP • Configure and verify NTP operating in a client and server mode • Explain the function of SNMP in network operations. • Describe the use of syslog features including facilities and levels.

Learning Outcomes and Credential Alignment *(cont.)*

	• Use commands to back up and restore an IOS configuration file. • IOS Image Management (Implement protocols to manage the network).
9. Explain how technologies such as virtualization, software defined networking, and automation affect evolving networks.	• Network Virtualization • Cloud Computing (Explain the importance of cloud computing). • Virtualization (Explain the importance of virtualization). • Virtual Network Infrastructure (Describe the virtualization of network devices and services). • Software-Defined Networking (Describe software-defined networking). • Controllers (Describe controllers used in network programming). • Describe controller-based and software defined architectures (overlay, underlay, and fabric). • Separation of control plane and data plane. • North-bound and south-bound APIs. • Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding). • Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible. • Interpret JSON encoded data.

ITAG Development Panel

Lead name	Institution/Organization	Role
Hamid Abdollahian	Cuyahoga Community College	Lead Panel Member
Kayleigh Duncan	Wright State University	Panel Member – Faculty
Kristi Hall	University of Cincinnati Clermont College	Panel Member – Faculty
Michael Kelley	Ohio University	Panel Member – Faculty
John McNamara	Stark State College	Panel Member – Faculty
Dovel Myers	Shawnee State University	Panel Member – Faculty
Ray Nejadfard	Cuyahoga Community College	Panel Member – Faculty
Dr. John Nicholas	University of Akron	Panel Member – Faculty
Patricia Opong	Columbus State Community College	Panel Member – Faculty
Tim Moore	Cuyahoga Valley Career Center	Panel Member – OTC Representative
Roy Pignatiello	Euclid City School District	Panel Member – Secondary Representative
Patrick Hoyer	Lubrizol Corporation	Panel Member – Industry Representative
Gabriel Koussa	PNC Bank	Panel Member – Industry Representative
Dr. Ben Parrot	Ohio Department of Higher Education	Senior Associate Director of Secondary Career-Technical Alignment Initiative Implementation
Nikki Wearly	Ohio Department of Higher Education	Director of Career-Technical Education Transfer Initiatives